Express Mail Label No.	Dated: _____

Docket No.: 20046/0201102-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Wieland Fischer et al.

Application No.: Not Yet Assigned

Confirmation No.:

Filed: Concurrently Herewith

Art Unit: N/A

For: METHOD AND APPARATUS FOR PROTECTING AN EXPONENTIATION CALCULATION BY MEANS OF THE CHINESE REMAINDER THEOREM (CRT)

Examiner: Not Yet Assigned

INFORMATION DISCLOSURE STATEMENT (IDS)

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 CFR 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement accompanies the new patent application submitted herewith.

A copy of each document on the PTO/SB/08 is attached. Pursuant to the Notice issued by the United States Patent and Trademark Office dated July 11, 2003 waiving the requirements of 37 C.F.R. 1.98(a)(2)(i), copies of the United States Patents on PTO/SB/08a are not submitted.

Citation BA is not in the English language. In accordance with 1.98(c), Applicant states:

The requirement for concise explanation of relevance of Citation BA is satisfied by the attached translations of the abstract (see MPEP § 609 A(3)).

In accordance with 37 CFR 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR 1.56(a) exists. In accordance with 37 CFR 1.97(h), the filing of this Information Disclosure statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 CFR 1.98 and the Examiner is respectfully requested to consider the listed documents.

The Commissioner is authorized to charge any deficiency of up to $300.00 or credit any excess in this fee to Deposit Account No. 04-0100.

Dated: April 15, 2004

Respectfully submitted,

FLYNN BARRESI

By _____ (53,970)

Laura C. Brutman
Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 753-6237 (Fax)
Attorneys/Agents For Applicant

PTO/SB/08a/b (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	Not Yet Assigned
Filing Date	Concurrently Herewith
First Named Inventor	Wieland Fischer
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	20046/0201102-US0

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	AA	US-5,991,415-B1	11-23-1999	Shamir	
	AB	US-6,282,290-B1	08-28-2001	Powell et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	BA	DE-100 24 325-A1	12-06-2001	Seysen		X

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	CA	Bong D et al: "OPTIMIZED SOFTWARE IMPLEMENTATIONS OF THE MODULAR EXPONENTIATION ON GENERAL PURPOSE MICROPROCESSORS"; Computers & Security, International Journal Devoted to the Study of Technical and Financial Aspects of Computer Security, Elsevier Science Publishers, Amsterdam, NL, Vol. 8, No. 7, 1 November 1989, Pages 621-630.	
	CB	Boneh D et al: "ON THE IMPORTANCE OF CHECKING CRYPTOGRAPHIC PROTOCOLS FOR FAULTS"; Advances in Cryptology, Eurocrypt, 11 May 1997, Pages 37-51.	
	CC	Schindler W: "A TIMING ATTACK AGAINST RSA WITH THE CHINESE REMAINDER THEOREM"; Cryptographic Hardware and Embedded Systems, 2nd International Workshop, CHES 2000, Worchester, MA, August 17-18, 2000 Proceedings, Lecture Notes in Computer Science, Berlin: Springer, Germany, Pages 109-124.	
	CD	Grossschadl J: "THE CHINESE REMAINDER THEOREM AND ITS APPLICATION IN A HIGH-SPEED RSA CRYPTO CHIP"; Computer Security Applications, 2000. ACSAC '00, 16th Annual Conference, New Orleans, LA, December 11-15, 2000, Los Alamitos, CA, IEEE Comput. Soc, 11 December 2000, pages 384-393.	
	CE	Schnorr C: "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS"; Lecture Notes in Computer Science, Vol. 434, Berlin, Springer, 1990, pages 239-252.	
	CF	Boneh D et al.:"ON THE IMPORTANCE OF CHECKING CRYPTOGRAPHIC PROTOCOLS FOR FAULTS"; Lecture Notes in Computer Science, Vol. 1233, Berlin, Springer, 1997, pages 37-51.	
	CG	Menezes A.J.: "HANDBOOK OF APPLIED CRYPTOGRAPHY"; Boca Raton, FL. CRC Press, 1997, pages 612-613.	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature		Date Considered	